IHIMS

Industrial Hygiene Information Management System

Questions or comments related to this plan should be directed to:

Contingency Plan Point of Contact:

Rick Daniel
Management Systems Support Division
Phone: 207-438-1681
Email: danielrd@mail.ports.navy.mil

Year 2000 Contingency and Continuity of Operations Plan (CCOP)

FOR

INDUSTRIAL HYGIENE INFORMATION MANAGEMENT SYSTEM (IHIMS)

Portsmouth VA 23502

Revised 15 MARCH 1999

TABLE OF CONTENTS

Section 1.0 EXECUTIVE SUMMARY

This IHIMS Year 2000 (Y2K) Contingency and Continuity of Operations Plan (CCOP) is written to help ensure the IHIMS 99 support for industrial hygiene data management is not adversely affected by year 2000 events. Year 2000 problems stem from the practice of using two digits instead of four digits ("98" vs "1998") to represent the year, resulting in the inability of computers and microprocessors to interpret 21st Century dates accurately. This problem is compounded by the fact that corrupted data can be perpetuated through interfaces to other information systems.

The IHIMS Program Office prepared this CCOP in response to DoD guidance, and to protect mission capability. This CCOP was developed as a stand-alone document because there is no existing CCOP that can be modified to address Y2K events.

This plan was developed as a compilation of DoD Y2K Management Plan, MHS Year 2000 Contingency and CCOP Planning Guide and Navy Guidance. Y2K contingency planning activities are prioritized based on their probability of occurrence and their potential impact to the navy mission.

Besides having a plan available to execute if Y2K events adversely impact IHIMS mission capability, one of the major benefits of developing this CCOP has been the exercise of identifying essential systems and work-arounds required to protect mission capability. This CCOP will continue to evolve as we gain more knowledge of potential Y2K event impacts. While this CCOP is intended to address the impact of Y2K events on the IHIMS 99 mission, much of it can be applied to other contingencies such as lightning strikes, tornadoes, earthquakes, etc.

Training for execution of the CCOP, and testing of CCOP implementation capabilities, will be through NMIMC with BUMED oversight and conducted prior to the implementation of IHIMS version 2.0 scheduled for August 1999.

Section 2.0 INTRODUCTION/PURPOSE

The purpose of this plan is to provide Year 2000 (Y2K) contingency planning information to all Navy locations in the event IHIMS is adversely impacted during the transition to the year 2000. It supports Department of Defense, Military Health System and Navy guidance. This Plan will be updated as needed and will remain in effect until rescinded by the IHIMS Program Office or BUMED.

Section 3.0 MISSION/SYSTEM DESCRIPTION

IHIMS is a relational database used to document and manage occupational health effects of hazardous operations to the people and environment within the naval community. IHIMS is designed to replace manual paper based processes, and to consolidate and standardize data about hazardous exposures so that it can be used for informed decision-making. In the event of complete system failure, those paper based processes could be reinstated, but the benefits of aggregating and standardizing data into useful information will be lost until the IHIMS is restored and that manual data is entered into the system.

Section 4.0 SCOPE

This plan covers all deployed versions of IHIMS within the naval community. It contains workarounds for support system failures such as power loss, Local Area Network failure, and personal computer/workstation failure. However, because they are base level responsibilities, this plan does not specifically address procedures for that infrastructure.

IHIMS 99 primarily supports industrial hygiene departments at naval facilities; both “child” and “parent” sites.

Section 4.1 ASSUMPTIONS

IHIMS is an application that utilizes Microsoft Access as a database and Delphi as a Graphical User Interface (GUI). The “system” consists of the application software, the database and GUI and the unidentified PC architecture a particular site has chosen to run the application on. It is assumed that each IHIMS System Administrator (SA) has properly ensured the Y2K certification of any hardware running this application. Based upon extensive testing by a third party and the subsequent certification of the software as being Y2K compliant, the project office estimates it to be a low risk system for Y2K related problems. The unknown variable and the primary vulnerability will be at the infrastructure (hardware, LAN and communications software internal to each site) level at each specific site deploying IHIMS and the commensurate risk associated with that infrastructure. The project office has no control over this variable but it is assumed that this will be appropriately handled at each site. IHIMS is a non-mission critical system, and in the

case of power loss or network communications failure, manual work around will clearly suffice until power and network communications are restored.

Section 4.2 COORDINATION ACTIVITIES

Once approved, this plan will be provided electronically to all prospective IHIMS sites by BUMED/NMIMC prior to the deployment of the software.

Section 4.3 REVIEW AND UPDATE PLAN

This CCOP will be updated prior to any planned update of IHIMS software (planned for 31 Aug 1999). It will remain a "living document" to keep pace with developments in system support requirements. The IHIMS System Program Office will approve updates to this plan before they are released electronically to using agencies.

Section 5.0: BACKGROUND

This document was written in concert with the Technology Management, Integration and Standards; Systems Contingency Plans – Review Criteria and Additional Guidance dated 11 March 1999 and provided by the Office of the Assistant Secretary of Defense (Health Affairs) Office of Information Management, Technology and Reengineering Technology Management, Integration and Standards Directorate Year 2000 Project Office.

This plan is provided to supplement IHIMS Y2k test documentation submitted to Health Affairs Contractor TMA on 12 January 1999 and 10 February 1999. That documentation provided test results and certification by a third party showing all IHIMS software to be fully Y2K compliant.

On 12 April 1999, the IHIMS Project Office was notified of the new Contingency Plan format and requirements document (referred to above and dated 11 Mar 99), and TMA requested that this Contingency Plan be rewritten to support those requirements.

The Year 2000 (Y2K) problem stems from the practice of using two digits instead of four (e.g. "98" vs. "1998") to represent the year, resulting in the inability of computers and devices to interpret 21st Century dates accurately. This problem becomes increasingly complex since

corrupted data can be perpetuated through interfaces with other information systems. Because of the widespread practice of using only two digits to represent the year in computer databases, software applications, and hardware chips, the potential exists for the failure of automated information systems (AIS) and infrastructure related items on or about 1 January 2000. This potential for failure is referred to as the "Y2K problem." Y2K related difficulties will arise when date cognizant devices attempt to sort or calculate using the year "00", not recognizing that the year is actually 2000. The resulting inaccuracies in date-related calculations could generate corrupt results and potentially cause systems to fail. Also, if erroneous data goes unrecognized, the problem could be perpetuated through interfaces (whether fully automatic or "air gapped" such as hand-carried disk or tape) to other systems. Some systems may have faulty logic that will not recognize the year 2000 as a leap year, leading to the incorrect calculation of the day of the week, for example. Other systems have triggers that are executed based on specific values of date fields, and still others have numeric overflow or rollover problems. The Y2K problem is unique in that our traditional CCOP plans and back-up systems may be effected by the same problem(s) as our primary systems - thus rendering them useless. In some cases, the Y2K problem may require a completely different method of accomplishing the mission. Over the past 50 years, the benefits of information technology (IT) have been applied to every aspect of our missions. In many cases, IT allows us to do our jobs better, cheaper, and faster than could be done without it. As the new century approaches, incorrect data generated by date-related processing could have detrimental effects on all information technology (IT) systems. Our challenge is to overcome the potential widespread failure of systems and equipment due to problems associated with processing date information associated with the year 2000.

Critical Dates (Midnight Crossings). The dates listed below constitute the minimum set of critical dates for IHIMS that have been identified and should be considered in the future when addressing potential year 2000 transition risks. IHIMS does not interface with other systems to receive or send date sensitive data. Nonetheless, it would be prudent to consider each of these dates critical.

- 8 Apr 1999 to 9 Apr 1999: The 9 Apr 99 Julian date represented by 9999 can be confused with some default programming codes and could cause processor errors.

- 8 Sep 1999 to 9 Sep 1999: The 9 Sep 99 date represented by 9999 can be confused with some default programming codes and could cause processor errors.
- 30 Sep 1999 to 1 Oct 1999: For the government calendar, this is the beginning of the fiscal year 2000.
- 31 Dec 1999 to 1 Jan 2000: This is the basic Y2K transition and the one that is most likely to cause a product or process to fail.
- 28 Feb 2000 to 29 Feb 2000: The year 2000 is also a leap year, although some systems may not recognize that. Systems may not perform the leap year calculation properly.
- 29 Feb 2000 to 1 Mar 2000: This time frame must be watched to ensure systems don't calculate a February 30th.
- 30 Sep 2000 to 1 Oct 2000: This time frame must be watched to ensure systems evaluate the fiscal change over properly.
- 30 Dec 2000 to 31 Dec 2000: The 365-366th day of the year 2000. Some processors may try to roll the date over to 1 Jan 2001.
- 31 Dec 2000 to 1 Jan 2001: This final risk period completes the leap year evaluation by establishing that the system "knows" that the year 2000 has 366 days.

Section 6.0 REFERENCE DOCUMENTS

DODD 3026.26, Continuity of Operations Policies and Planning, 26 May 1995

OSD(HA) MHS Year 2000 Contingency and Continuity of Operations Planning Guide, 1 Oct 1998

Technology Management, Integration and Standards; Systems Contingency Plans – Review Criteria and Additional Guidance dated 11 March 1999

Section 7.0: COMPLIANCE ASSURANCE REVIEW METHODOLOGY

This contingency plan addresses the following areas in order to ease the review by the ASD(HA) IV & V Teams' review of contingency scenarios involving IHIMS and validating that plan against DoD guidelines. Each of these areas is addressed individually in accordance with DoD and MHS documentation.

Systems Contingency Plan Review Areas:

1. Identification of Risks
2. Trigger Definition
3. Alternate Procedures
4. Zero Day Strategy
5. Preserve Data (i.e. Backup and Restore Procedures)
6. Resource Planning

7. Problem Reporting Instructions/Contacts

The IHIMS Project Team has attempted in good faith to follow guidelines given in the DoD Year 2000 Management Plan (version 2, 14 Oct 1998) and the MHS Guide.

Section 8.0: CONTINGENCY PLAN REVIEW AREAS:

8.1 Identification of Risks

This plan identifies risks at the system level. These risks were also addressed in the Assessment Phase of Y2K preparation for IHIMS. Risk identification and trigger definition are the core of this contingency plan since they define at the lowest level of use, what may result from Y2K related hardware/software failures and what may cause such failures.

Risk assessment is the first step in preparing the system element of the AIS contingency plan. It is conducted in three stages:

1. Identify risks. The identification, under the system contingency plan, involves the analyses of risks that might inhibit the AIS project managers' ability to identify, report, analyze, repair, test, and distribute system repairs to the user community.

2. Determine the probability of occurrence (P^o) and consequences of occurrence (C^o). Once a set of risks or hazards is identified, the P^o and C^o are subjectively determined and rated as a low, medium, or high risk.

3. Determine the risk classification (RC). Risk classification is determined by multiplying P^o and C^o. General rules for arriving at risk classification are contained in the following Table.

Risk Classification Guidelines

P^O	TIMES	C^O	EQUALS	RC
Low	X	Low	=	Low
Low	X	Medium	=	Medium
Low	X	High	=	Medium to High
Medium	X	Low	=	Low
Medium	X	Medium	=	Medium
Medium	X	High	=	High
High	X	Low	=	Low to Medium
High	X	Medium	=	Medium to High
High	X	High	=	High

Based upon the above analysis of probability of occurrence and the corresponding consequence of occurrence related to Y2K initiated software problems, the below table of risks has been established for IHIMS. Since this Contingency Plan can addresses IHIMS Y2K failures from a navy wide, systemic perspective, it is incumbent upon each individual, local system administrator and Information System Security Officer (ISSO) to ensure local safeguards are in

place to continue operations in the event of local system failure. Those plans should use this contingency plan as a basis for planning for such events. Please note the below table of risks:

MHS System-Level AIS Contingency Plan For IHIMS 99 Operation					
Normal Operating Procedures	**Risk**	**P^0**	**C^0**	**RC**	**Contingency Operations Mode**
Problem Identification					
1. User reports problem by calling local IHIMS system administration.	Local administrator unable to resolve.	L	M	M	User implements manual operating mode pending problem resolution.
2. System Administrator reports problem to IHIMS 99 Help Desk.	IHIMS 99 Help Desk unable to resolve.	L	L	L	User implements manual operating mode pending problem resolution.
3. IHIMS Help Desk reports problem to contractor Program Manager, for investigation.	Contractors unable to quantify problem.	L	L	L	User implements manual operating mode pending problem resolution.
Problem Analyses					
1. AIS Project staff resolves problem, provides fix guidance to site.	Project staff unable to resolve problem.	M	H	H	Activate contractor/vendor support IAW statements of work/delivery orders.
2. AIS Project Office refers problem to vendor.	Vendor unable to solve problem in a timely manner.	L	M	M	Implement contract/delivery order to conduct problem analyses. Use vendor developmental environment, as arranged.
3. Coordinate non-software problems with contractors/vendors, other AIS projects, TIMPO, and MTF staff.	Failure of outside party to accept problem ownership or co-ownership.	M	M	M	Implement problem escalation procedures in MOU/A(s). Clearly define what constitutes problem ownership/co-ownership in MOU/As.
4. Determine if problem is caused by hardware, system software, or local/wide area communications.	Failure to identify problem cause by AIS PM.	M	M	M	Implement contract/delivery order to conduct problem analyses. Use vendor developmental environment, as arranged.
Software Repair/Problem Resolution					
1. AIS Project Office repairs problem, provides fix to user.	Unable to resolve, not an AIS problem	M	M	M	Exercise joint agreements with interfacing organization/project.
2. AIS Project Office repairs problem, provides fix to user.	Unable to resolve, hardware problem	M	M	M	Exercise pre-existing written agreements with hardware vendor to repair and distribute/deploy repair.
3. AIS Project Office repairs problem, provides fix to user.	Unable to resolve, local/wide area communications problem.	M	M	M	Implement agreement(s) with TIMPO/vendor to resolve problem. Implement agreement to use contractor resources. Implement on-site problem resolution procedures.
4. AIS Project Office repairs problem, provides fix to user.	Unable to resolve, system SW issue.	M	M	M	Exercise repair agreement(s) with vendor(s) to affect repair.
Software Distribution					
1. AIS Project Office distributes software fix electronically if possible, otherwise, via U.S. Mail distribution of diskette/CD-ROM.	U.S. Mail too slow to meet distribution requirements.	L	L	L	Express mail option, as appropriate. Validate data recovery procedures during testing, and include instructions for data recovery.
2. Hardware fix implemented by vendor.	Vendor is overrun with Y2k problems.	M	H	H	Exercise agreement(s) for vendor(s) or alternate sources to conduct on-site repair and implementation.

8.2 Trigger Identification

This CCOP will be executed for any serious degradation of mission capability related to Y2K failures. If there are any serious service disruptions affecting mission accomplishment, the affected organization will promptly notify the IHIMS helpdesk, 1-301-295-0042, to assist in assessment of the degradation. Trigger events or system indicators that may require activation of this plan include erratic system results, system degradation, corrupt data, or catastrophic failures. For each of the critical Y2K dates listed above, each base's IHIMS system administrator will check system functions and judge the results of their performance. If problems are suspected, the base level system administrator will notify the IHIMS Help Desk for assistance in evaluating actual damage, determining any corrective action required, and notifying all effected parties. The IHIMS Help desk will contact the Navy IHIMS Program Management Office for approval to implement corrective actions at base level, especially if the corrective action will be required at all IHIMS sites.

8.2.1 Exit Criteria (Returning to Normal Operations)

Returning to normal operations would normally occur when the AIS project office and/or other organization has repaired the system (or system element), completed the repair at the operating site and provided instructions for resuming normal operations. Reinstating normal operations typically involves some or all of the following actions:

- Data recovery (which may involve recapturing data recorded manually during the contingency operating period.
- Locally testing the AIS (or other system element) to ensure normal operations have been achieved by the system element repair (directions are provided by the AIS project office should local testing be necessary).
- Assuming normal operations by notifying all parties involved that manual operations have ended and normal automated operations will be begin at a specified (and coordinated) time.

8.2.2 Continuity of Operations Plan

The Continuity of Operations Plan addresses triggers or possible failure modes that could impact system operation and mission accomplishments. It focuses more directly on user needs and specific work arounds for these failure modes. Subject headings for the plan are:

Process/Function. This identifies a particular function within the system, such as data processing, communication, or information presentation.

Risk/Probability of Occurrence/Consequences/Risk Classification. These columns identify contingency hazards or risks that are addressed in the plan within each Process/Function. Risk assessment is the first step in preparing the system element of the AIS contingency plan. It is conducted in three stages:

Risk Classification Guidelines

P^O	TIMES	C^O	EQUALS	RC
Low	X	Low	=	Low
Low	X	Medium	=	Medium
Low	X	High	=	Medium to High
Medium	X	Low	=	Low
Medium	X	Medium	=	Medium
Medium	X	High	=	High
High	X	Low	=	Low to Medium
High	X	Medium	=	Medium to High
High	X	High	=	High

Pre-Contingency Planning. This column addresses things to be done before the contingency to reduce the risk and help in preserving mission capability.

Contingency Execution. This column identifies the procedures to be used if the contingency occurs and your system is impacted. It also focuses on maintaining mission capability.

Post Contingency Recovery. This column establishes procedures for returning systems to an "on-line" status.

Resources. This is a summation of resources required to reduce risk prior to contingencies, execute contingency operations, and recover from contingency operations, including bringing systems back on-line in a normal operating mode. Resources may include such categories as funding, personnel, and equipment.

Process/Function	Hazard	Probability	Impact	Score	PreContingency Planning	Contingency Execution
Total System Failure	Power Loss or Catastrophic System Loss	M	H	H	• Practice standard data backup procedures • Make XX day supply of hardcopy forms	• Manual Operations • Manually fill out forms or revert bac to Y2K Compliant version of old IHIMS.
Partial System Failure	LAN Failure • Hub • Router • Firewall • File Server failure • Etc.	M	H	H	• Practice standard data backup procedures • Identify critical data entry forms • Make 30 day supply of hardcopy critical forms	• Users who cannot access the forms may contact the IHIMS S to install a temporary copy of the forms directly on their PC c Commence Manual Operations. • Users who cannot access the database server must commen manual operations.
	Client PC Failure	M	L	L	• Option 1: Use another compliant PC • Option 2: Treat as Total System Failure	• Identify Compliant PCs

Process/Function	Hazard	Probability	Impact	Score	PreContingency Planning	Contingency Execution
Interface Failure	No automated interfaces are planned for IHIMS at this time. However, some sites may choose to manually load electronic data from other sources.	L	L	L	• Individual sites determine local requirements for physically uploading/ downloading any electronic data and devise data. Execute upload interfaces the evening before critical midnight crossings to ensure most current data is available for continued operations.	• For personnel data, enter any critical changes manually through the demographics screen form .
Limited/partial loss of system functionality	Certain input screens within IHIMS 99 do not work	L	L	L	• Have manual mode of operation in place to continue operations while software technicians correct issue.	• Commence manual mode only for those input screen forms th do not work.
	Certain output reports within IHIMS do not work	L	L	L	• Run critical output reports (locally determined, but consider at least the Risk Assessment Report) just prior to critical midnight crossings, to have most current data available	• Notify the IHIMS 99 Help Desk ASAP wi specifics of the problem.
System-wide degraded performance or excessive system delays	LAN performance degraded	M	L	L	• If network is too slow to use, consider commencing manual operations.	• Notify appropriate base comm personne

Section 8.3 ALTERNATE PROCEDURES

Local IHIMS System Administrators (SA) will establish procedures to ensure that in the event their IHIMS software or in-house hardware experiences any kind of Y2K disruption, an alternative system or procedure is available in order to continue the functional appropriate business process until the system is restored.

Plans should include technical workarounds necessary to recover the system or use other system capabilities to meet the customer's requirement to sustain mission critical capabilities. This may include the use of the older, original IHIMS (Y2K version). It may include the use of manual record keeping practices as outlined within the navy's field industrial hygiene Field Operations Manual (IHFOM) and OPNAV Instruction 5100.23E. It may also include a combination of automation and manual processes.

Section 8.4 ZERO DAY STRATEGY & PRESERVING DATA

The zero day strategy involves identifying those actions that will be taken before and during critical Y2K date transitions to mitigate consequences of Y2K contingencies.

The site specific zero day strategy might include transition preparation steps such as:

1. Minimizing leave for key personnel, pre-positioning personnel, and recalling key personnel;
2. Risk mitigation procedures such as running "end-of day" procedures earlier in the day;
3. Taking systems off-line for date transition (zero day) periods (if feasible);
4. Verifying good data back-up products before critical crossing dates;
5. Printing hard copy products before critical crossing dates;
6. Preparation for proactive "health analysis" steps to be carried out at 'zero day', such as reviewing user screens for Y2K problems, validating full system functionality, entering date-sensitive test data and verifying the system produces expected results, etc.;
7. Establishing Y2K response and reporting teams above and beyond normal help desk and problem resolution staffing.
8. Establishing and/or distributing instructions and procedures for returning to normal operating mode, after a Y2K related contingency has been invoked.

The degree of zero-day planning necessary for each system is a function of the local System Administrator's (SA) overall responsibility for Y2K oversight. Complexity and the degree of potential consequences resulting from an unanticipated systems failure will be minimal since the majority of IHIMS systems will be on stand alone PCs which can readily be replaced with hardware operating optional software.
Most IHIMS PCs and servers are not backed up by uninterruptable power supplies (UPS). Each base must assess their confidence that power systems will not fluctuate during critical midnight crossings. For any midnight crossing date where confidence is not high that power systems will

be stable, the server shutdown procedures should be executed prior to the midnight crossing, and the server should not be brought back on line until power and network communications are determined to be stable, after the crossing.

Section 8.5 RESOURCE PLANNING

The Program Sponsor of IHIMS (BUMED) and the Functional Sponsor (BUMED) will cooperate to ensure financial resources exist to quickly resolve any Y2K issues that may arise as a result of the navy's use of IHIMS. Both organizations will work with the IHIMS Project Office to ensure funding is on hand for such emergent requirements. It will be the Project Office's responsibility to ensure technical personnel are on hand to assist with any perceived problem. These responsibilities may/may not include the following tasks:

1. Estimating the resources (e.g., time, money, test environment, and contractor/vendor resources) required to correct problems encountered.

2. Developing memoranda of understanding/agreement (MOUs/MOAs) with organizations that will support issue resolution involving Y2K related problems.

3. Estimating the resource requirements for handling system repair and restoration under worst-case failure scenarios.

4. Extending or initiating contracts/delivery orders with contractors/vendors to ensure adequate human resources and repair response times are included.

5. Descriptions of any response teams that will be deployed to correct system problems if appropriate (staffing).

6. Hardware and/or software that is needed/acquired/requisitioned specifically to prepare for Y2K contingencies.

Section 8.6 PROBLEM REPORTING/CONTACTS

Roles and Responsibilites

Base Level. The IHIM System Administrator (SA) is responsible for ensuring that data backups are performed just prior to close of the last business day before each critical midnight crossing. As a precaution the SA will follow procedures to gracefully power down the IHIMS server prior to close of business on 31 December 1999, and bring the system back up after the new year when power systems and network communications are stable. Each base SA should assess the local risk of power systems failure for critical midnight crossings other than 31 December 1999, and power down the server for any crossings where confidence is not high that power systems will not fail. Each base should determine the amount of forms required for manual operations. They

should also determine reasonable plans for reverting back to the Y2K compliant version of the old IHIMS if that course of action is preferred.

Navy IHIMS 99 Project Office. MSSD will work with NMIMC and BUMED to ensure contractors have remote access to the IHIMS servers through firewalls for remote maintenance on 4 January 2000 after any site identifies such a need in writing via BUMED and NMIMC.

Contractor System Program Office. The contractor will have the IHIMS Help Desk up, ready to assist (over the phone) in performing data backups, shutting down IHIMS systems, and bringing IHIMS systems back on line after 4 January 2000. This will be contingent upon continued funding in advance to support the necessary resources.

POINTS OF CONTACT

IHIMS Project Manager:	Dennis Smoot Naval Environmental Health Center (NEHC) Portsmouth, VA 23502 (757) 462- 5523
IHIMS Help Desk:	Naval Environmental Health Center (NEHC) Dennis Smoot (757) 462-5523
IHIMS Developers:	NEHC

RESPONSE TEAM

There will be no organic response team formed for any of the critical midnight crossings. Prior to the 31 Dec 1999 crossing, IHIMS PCs and servers should be powered down, and not brought up until after the new year and power and network systems have stabilized. The IHIMS Help Desk will be available via telephone or e-mail to aid as required to bring the IHIMS application back on line once the local hardware infrastructure has been stabilized.